Cloud Forensics

Carlo Dumit
Erick Sousa
Rafael Padilha
Ricardo Menzer

Seminar Series

MO447 - Digital Forensics

Prof. Dr. Anderson Rocha
anderson.rocha@ic.unicamp.br
http://www.ic.unicamp.br/~rocha

Outline

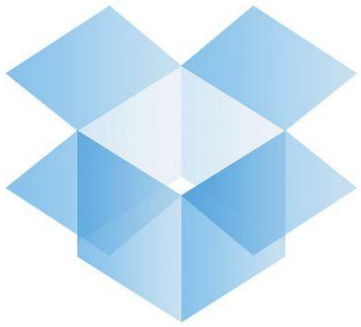
Outline

- Introduction
- Aspects of Cloud Forensics
- Challenges
- Opportunities
- Conclusions
- References

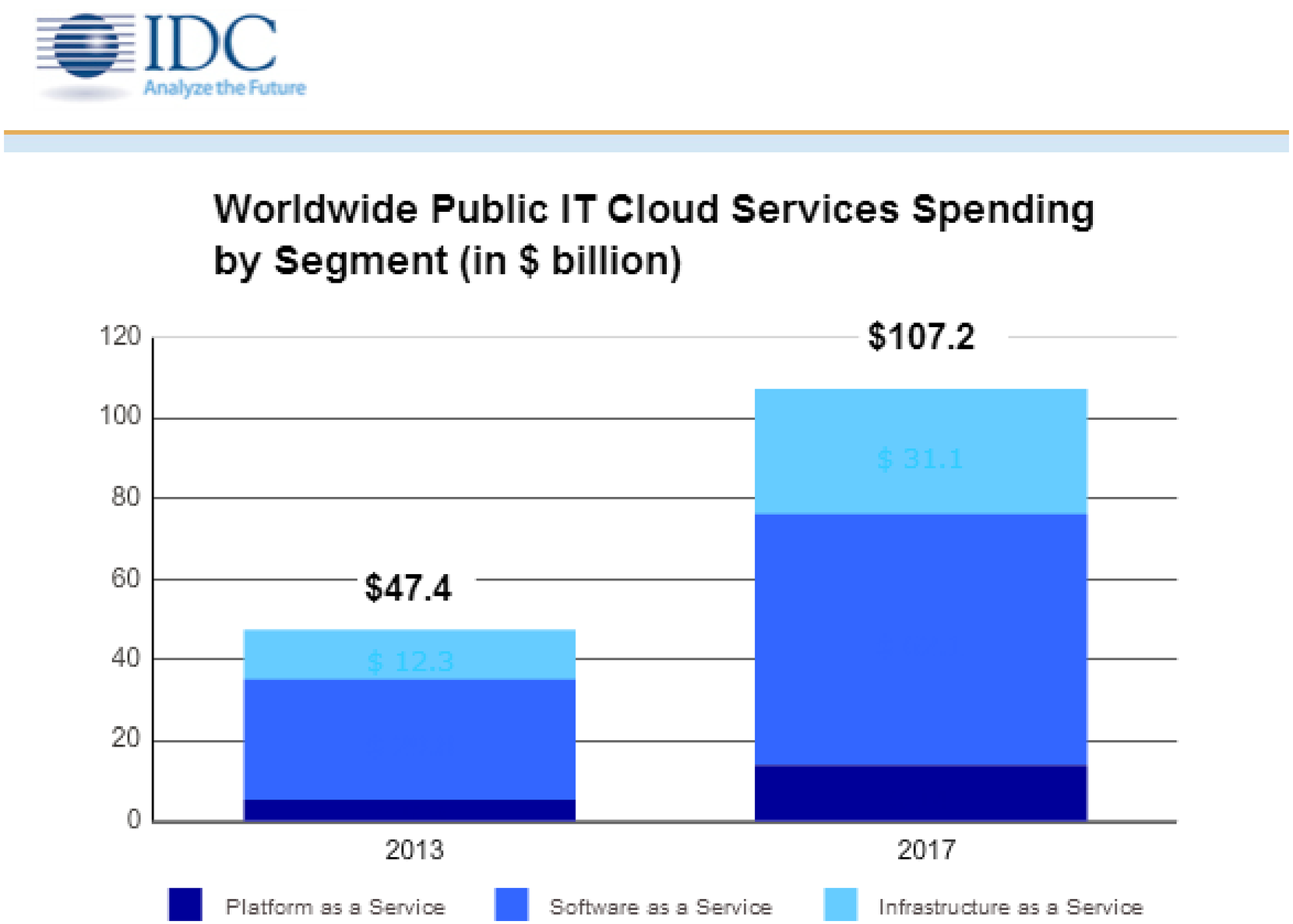
Introduction

Cloud Computing

- A model that enables convenient, on-demand network acess to a shared poll of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal Cloud Service Provider (CSP) interaction
- Examples:



- Worldwide spending on public IT cloud services is predicted to reach $107 billion in 2017

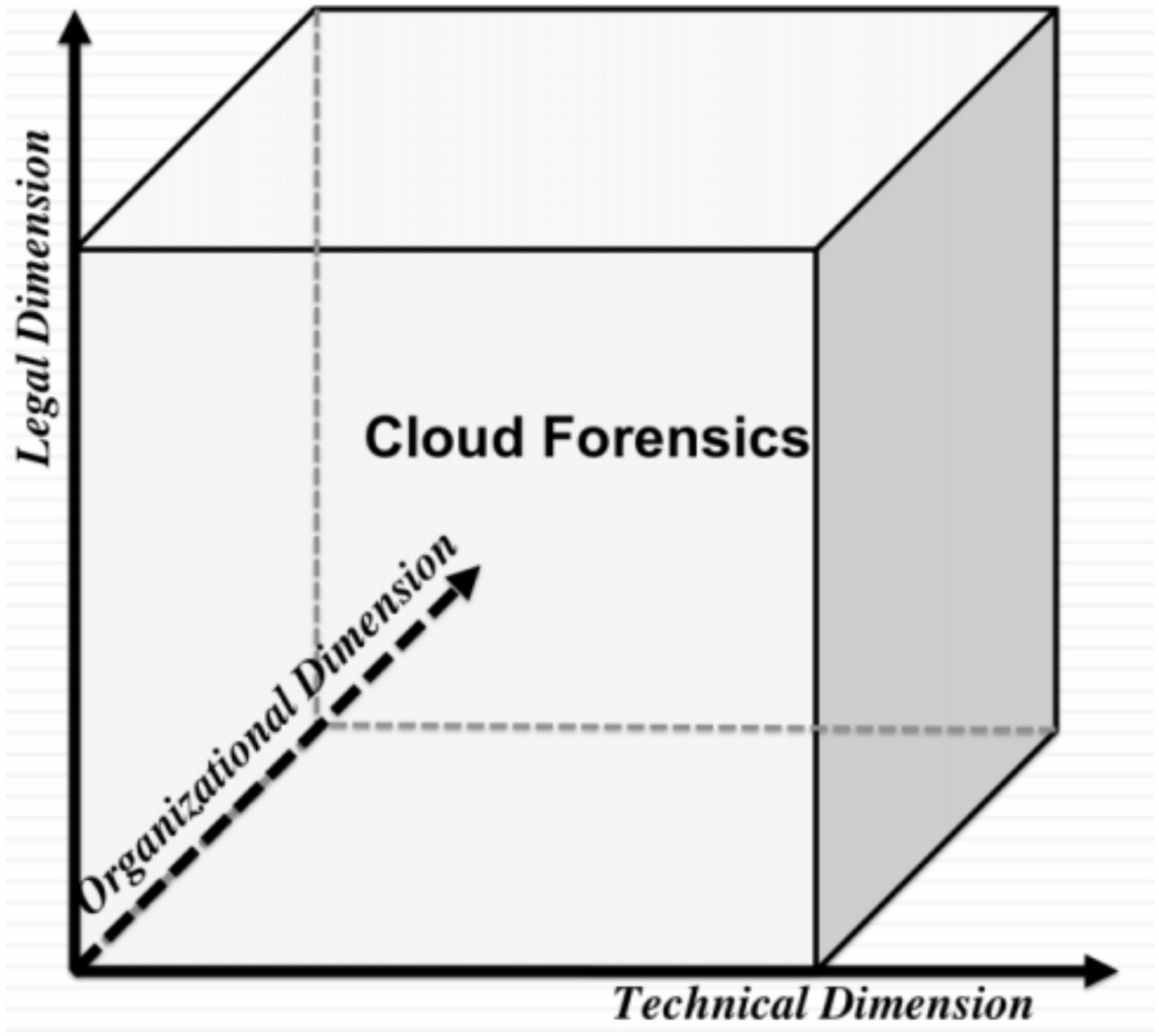


© International Data Corporation (http://www.idc.com/getdoc.jsp?containerId=prUS24298013)

Cybercrimes and Cloud Crimes

- Cybercrimes involving the cloud increase just like the investments on cloud services
- Cybercrimes has outgrown Drug Dealling as a global crime, costing U$ 105 billion per year
  - Hacker may use a Cloud Server to do a DoS attack or to share child pornography. Whose fault is it?
  - What if the hacker lives somewhere where what he is doing is not considered a crime, but where the CS is located it is?

- Cloud Forensics is a multi-dimensional issue, instead of merely a technical one



© Keyun Ruan (http://www.ruankeyun.com)

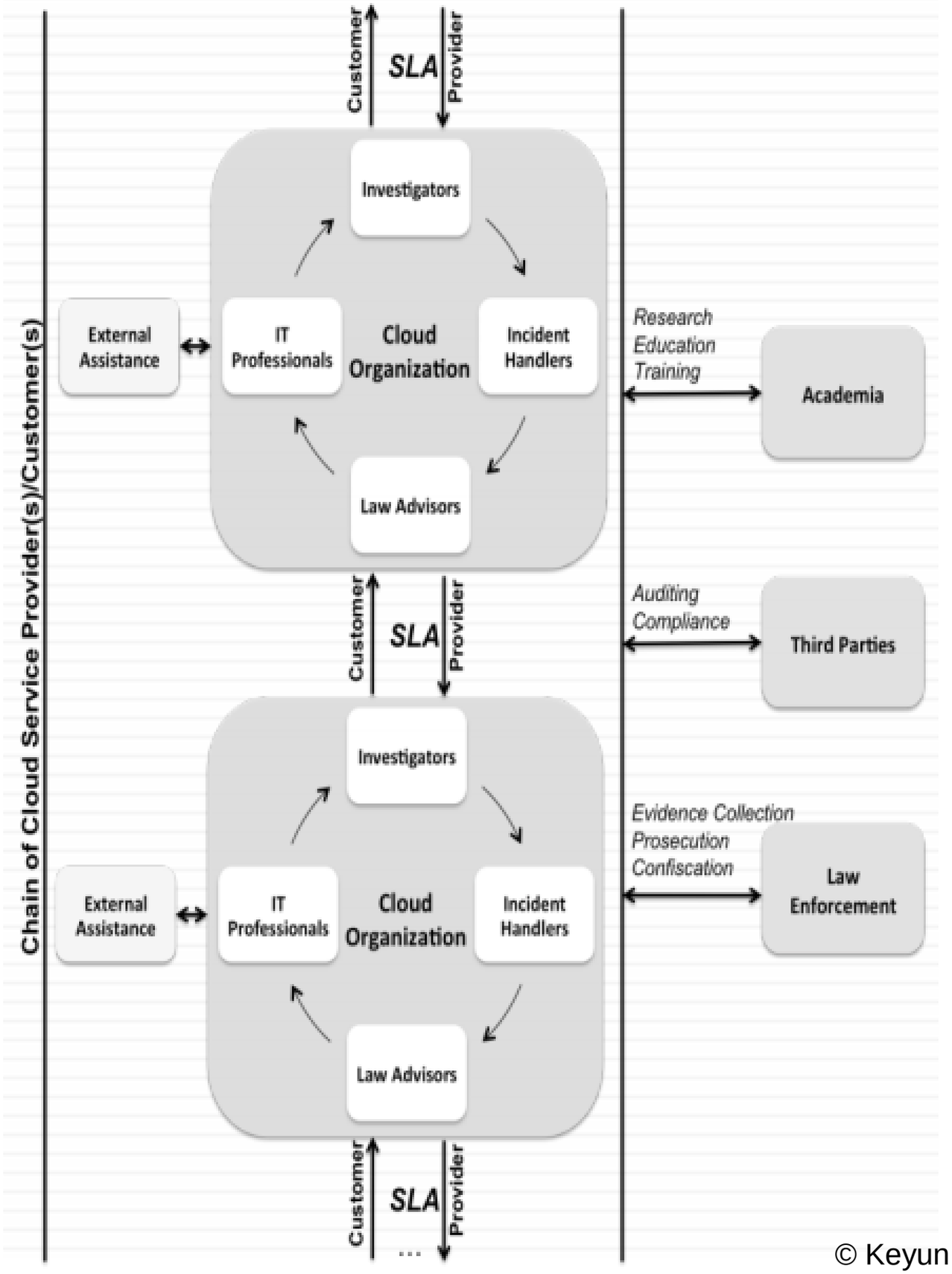
Technical Dimension

- Procedures and tools needed to perform the forensic process in a cloud computing environment
- E.g., data collection, evidence segregation, live forensics and proactive measures

Organizational Dimension

- A forensic investigation in a cloud computing environment involves at least two entities:
  - Cloud Service Provider (CSP)
  - Cloud Costumer
- The CSP may outsource services to other parties, widening the scope of the investigation

...

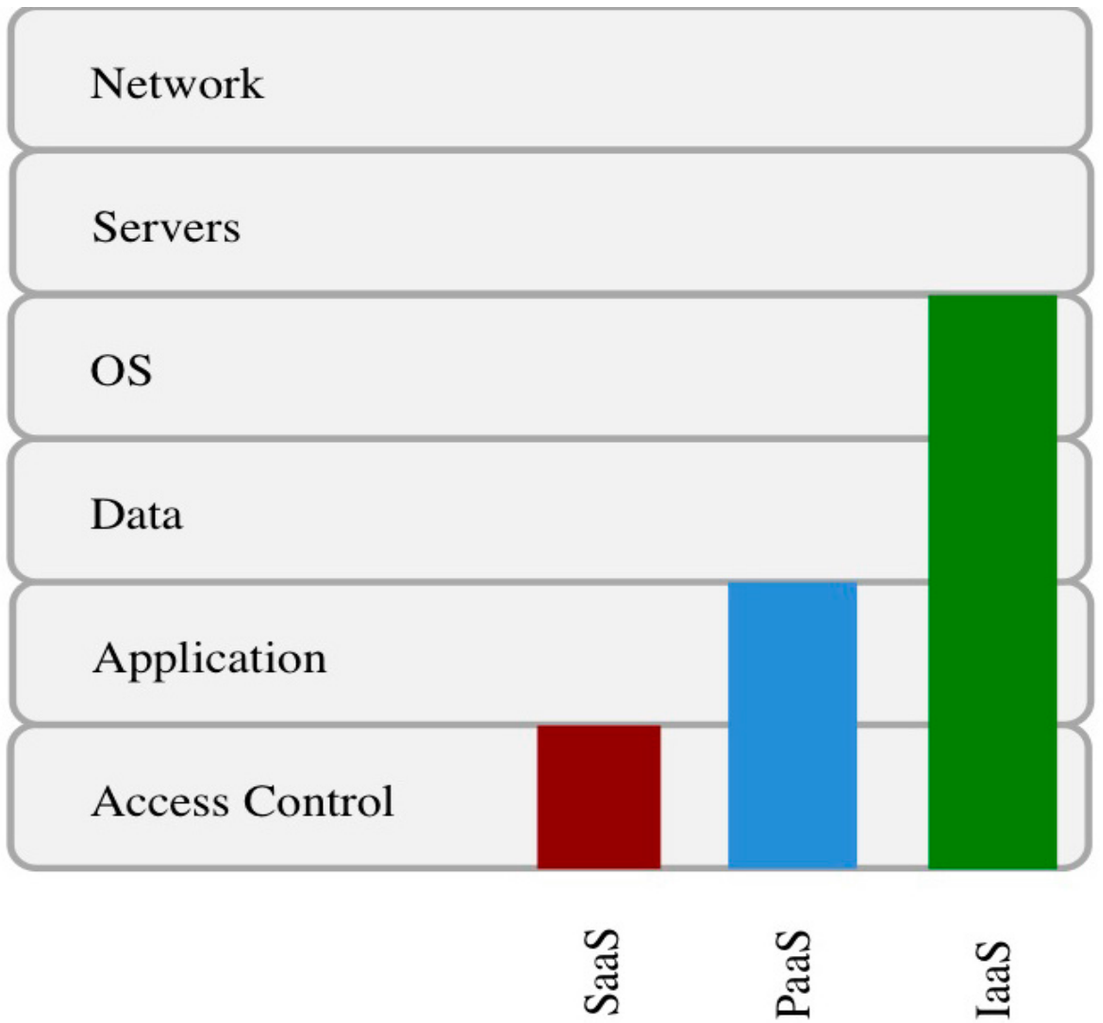


Legal Dimension

- Multi-jurisdictional and multi-tenancy challenges are the top legal concerns
- Forensic activities must not breach laws and regulations in the jurisdictions where the data resides
- Also the confidentiality of other tenants that share the same infrastructure should be preserved
- Defined by the Service Level Agreements (SLAs)

Cloud Services

- SaaS (Software)
- PaaS (Platform)
- IaaS (Infrastructure)



[Zawoad 2009]

SaaS – Software as a Service

- “on-demand software”
- Ex: Google Mail, Office 365
- Customer does not have any control of the underlying operating system
- Forensic Data:
  - Logs provided by CSP
  - Client Browser

PaaS – Platform as a Service

- Environments to deploy applications
- Ex: Google App Engine, Heroku
- Customer has no control over underlying environment
- Forensic Data:
  - Logs provided by CSP
  - Recommended: encrypt logs and tranfer to third party storage

IaaS – Infrastructure as a Service

- Customer has control of Virtual Machine provided by CSP
- Ex: AWS EC2, Windows Azure, Rackspace
- Forensic Data:
  - Snapshots (forensic images)
  - Volatile Data
  - Virtual Introspection

Possible problems

- Loss of data
  - User makes ilegal use of Cloud Service (i.e. Spam)
    - Shutdown VM
    - Cancel contract with CSP
- Lack of evidence
  - User claims VM was compromised

Challenges

Forensic Data Collection

- Process of identifying, labeling, recording and acquiring forensic data.
- Should not breach laws or regulations in the jurisdictions where data is collected
- Should preserve the segregation between tenants

Forensic Data Collection

- Varies according to cloud model, but highly dependent on CSP.
- CSP hide data location to facilitate data movement and replication.
- Many CSP do not provide tools to help forensic investigations
  - IP Logs of client access
  - Virtual Machine and Disk Images

Live Forensics

- Issues:
  - Mobile endpoints and time/geographical differences difficult timeline reconstruction
  - Huge volume of different log formats
  - How to handle deleted data
- Challenges: to recover the deleted data, identify and use it for event reconstruction in the cloud

Evidence Segregation

- Different instances running on a single physical machine are isolated from each other via virtualization
- Need to separate “neighbors”
- Logs collect data from multiple tenants
- Challenge for CSPs and law enforcement agencies to segregate resources during investigations without breaching the confidentiality of other tenants

Evidence Segregation

- Easy-to-use feature of cloud models contributes to a weak registration system (anonymity)
- Lack of standards when dealing with encryption
- Need for agreement between CSP, consumers and law enforcement agencies.

Virtualized Environments

- Data and computational redundancy
- Redundancy is achieved using virtualization (virtual machines – VM)
- Instances of serves running as VMs monitored by Hypervisors (can be SW, FW or HW)

Virtualized Environments

- Hypervisors:
  - Targets of attacks
  - Lack of policies, procedures and techniques for forensics investigations

Virtualized Environments

- Data mirroring in different jurisdictions
- Lack of transparent, real-time information of data locations => Law and regulations violation
- CSPs cannot provide a precise location of a piece of data.
- Need of strong international cooperation

Internal Staffing

- Conventional networking techniques used in cloud forensics
- Lack of technical and legal expertise makes cloud forensics a big challenge
- Cloud technology evolves much faster than forensics research, laws and regulations

External Dependency Chains

- CSPs have dependencies on other CSPs
- Cloud Forensics investigations needs to investigate every link in the dependency chain
- Procedures, policies and agreements related to cross-provider forensic investigations are virtually nonexistent

Service Level Agreements

- SLAs omit important terms regarding forensic investigations: low customer awareness, limited CSP transparency and lack of international regulation.

Multiple Jurisdictions and Tenancy

- Multiple jurisdictions and multi-tenancy are a significant challenge to cloud forensic investigations
- Different requirements regarding data access and retrieval, evidence recovery, admissibility and chain of custody
- Absence of a world wide regulatory entity impacts cloud forensics investigations

Opportunities

Cost Effectiveness

- Reduces IT costs
- Very attractive to small and medium enterprises

Data Abundance

- Data is replicated through many servers
- Reduces data degradation (e.g. bit rot) and data loss
- Very unlikely that a vital data is completely destroyed

Overall Robustness

- Common techniques are applied to increase data robustness:
  - MD5 hash
  - Versioning
  - Log access

Scalability and Flexibility

- Cloud Services provides an almost unlimited storage
- More information is stored inside logs

Policies and Standards

- Cloud Computing is a new field of opportunity
- Great time to lay foundations

Forensics as a Service

- Specialized services to aid on investigating, and crime solving
- Anti-Virus in the Cloud

Personal Motivations

- Challenging field
- Requires creative solutions

Personal Motivations

- Challenging field
- Requires creative solutions

- … And very profitable!

Personal Motivations

- Average salaries (year wage):
  - USA: $43.000 - $100.000 (U.S. Dollars)
  - UK: $44.000 - $117.000 (U.S. Dollars)
  - Brazilian Federal Police: R$ 168.000

Conclusions

Conclusions

- Cloud Forensics is a very recent field that some describe as a ticking-time bomb
- It still requires a lot of research and, more importantly, an international effort between countries and their law enforcers
- However, it also provides great opportunities that Digital Forensic may take advantage of
- Besides being very profitable for those interested in it

References

References

- ***P.Mell and T. Grance**, The NIST Definition of Cloud Computing, Version 15, 2009.*
- ***Federal Bureau of Investigation**, Regional Computer Forensics Laboratory, Annual Report for fiscal Year 2007, Washington, DC (www.refl.gov/downloads/documents/RCFL_Nat_Anuual07.pdf), 2007*
- ***Jon Shiring**, Respawn Entertainment. Let's talk about the Xbox Live Cloud (http://www.respawn.com/news/lets-talk-about-the-xbox-live-cloud/), 2013*
- ***Zawoad, S., Hasan, R (**2013). Digital Forensics in the Cloud (CrossTalk Magazine)*
- ***Birk, D., Wegener, C** (2011). Technical Issues of Forensic Investigations in Cloud Computing Environments*
- ***Ryan Corey**, TrainACE. The Average Salary of a Computer Forensics Career and the EC-Council CHFI Certification(http://www.trainace.com/the-average-salary-of-a-computer-forensics-career-and-the-ec-council-chfi-certification/)*
- ***Centro de Seleção e Promoção de Eventos**, UnB. Concurso Público para Perito Criminal (http://www.cespe.unb.br//concursos/dpf_12_perito/)*

Thank You!

Obrigado!